

APPROVED	O.G. FIG.
	CLASS SUBCLASS
DRAFTSMAN	

FIG. 1

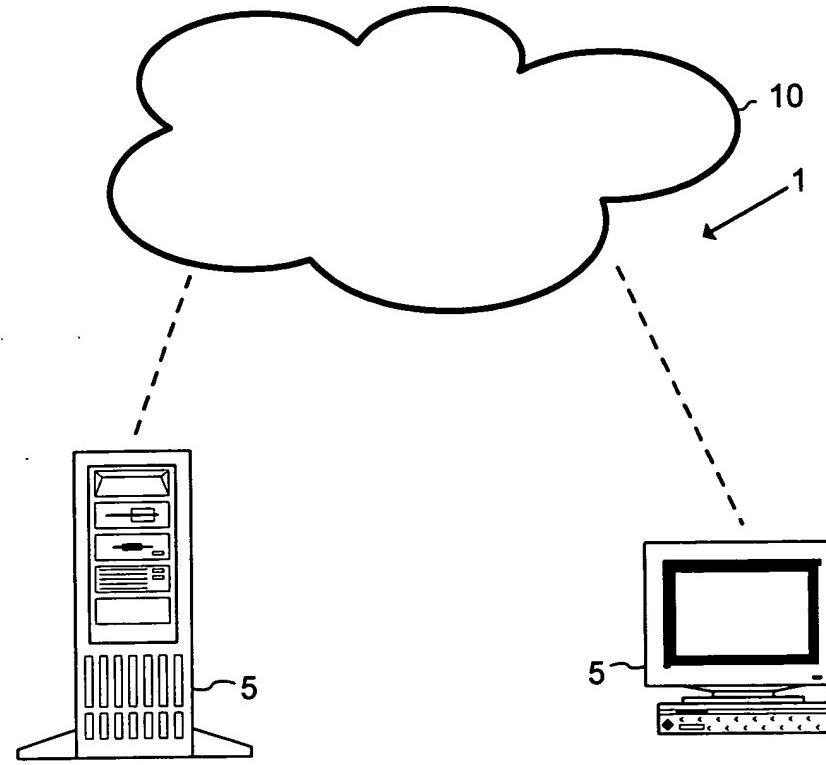
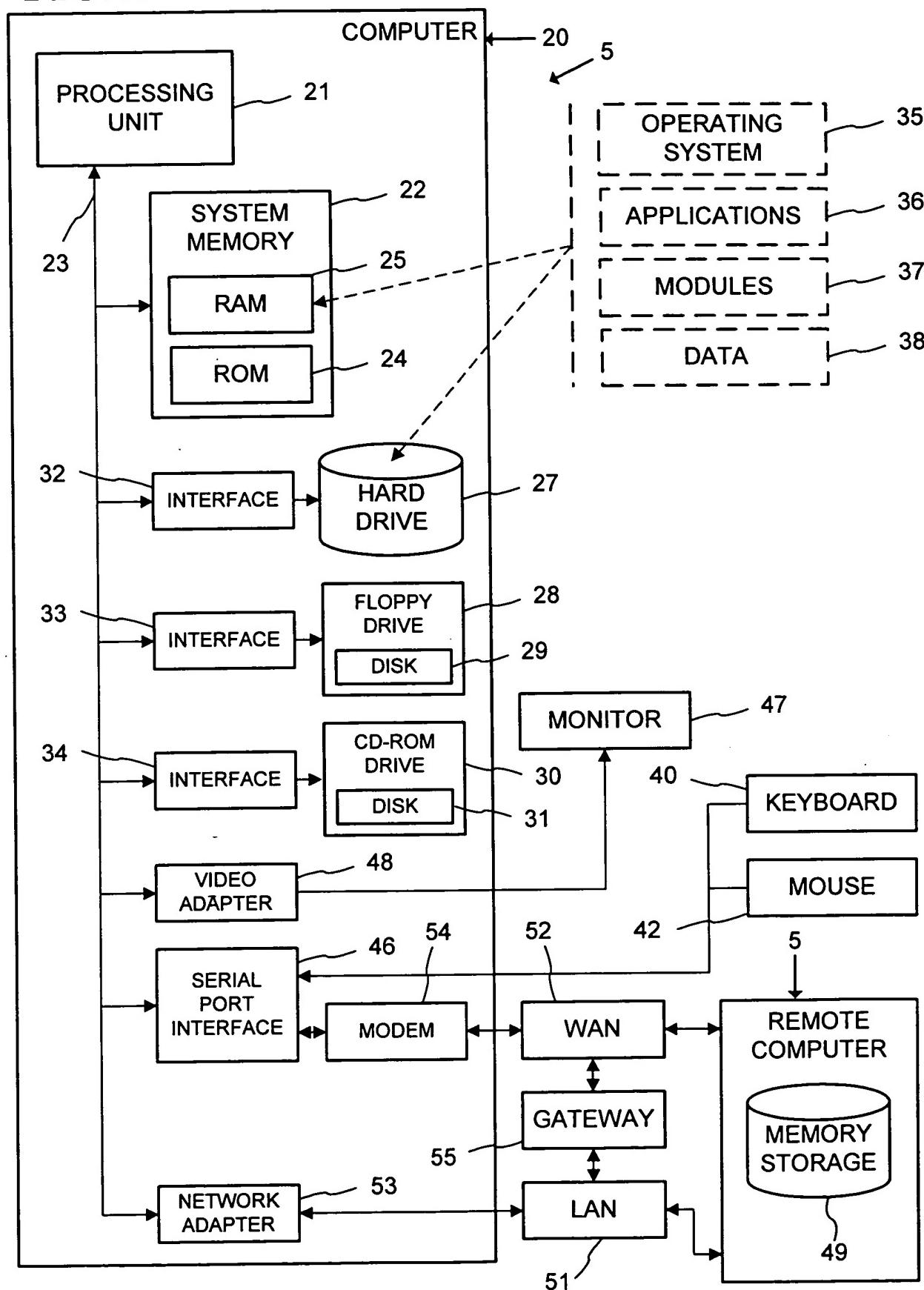


FIG. 2



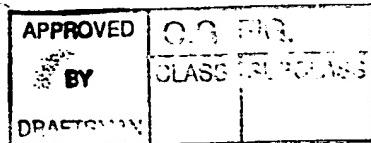
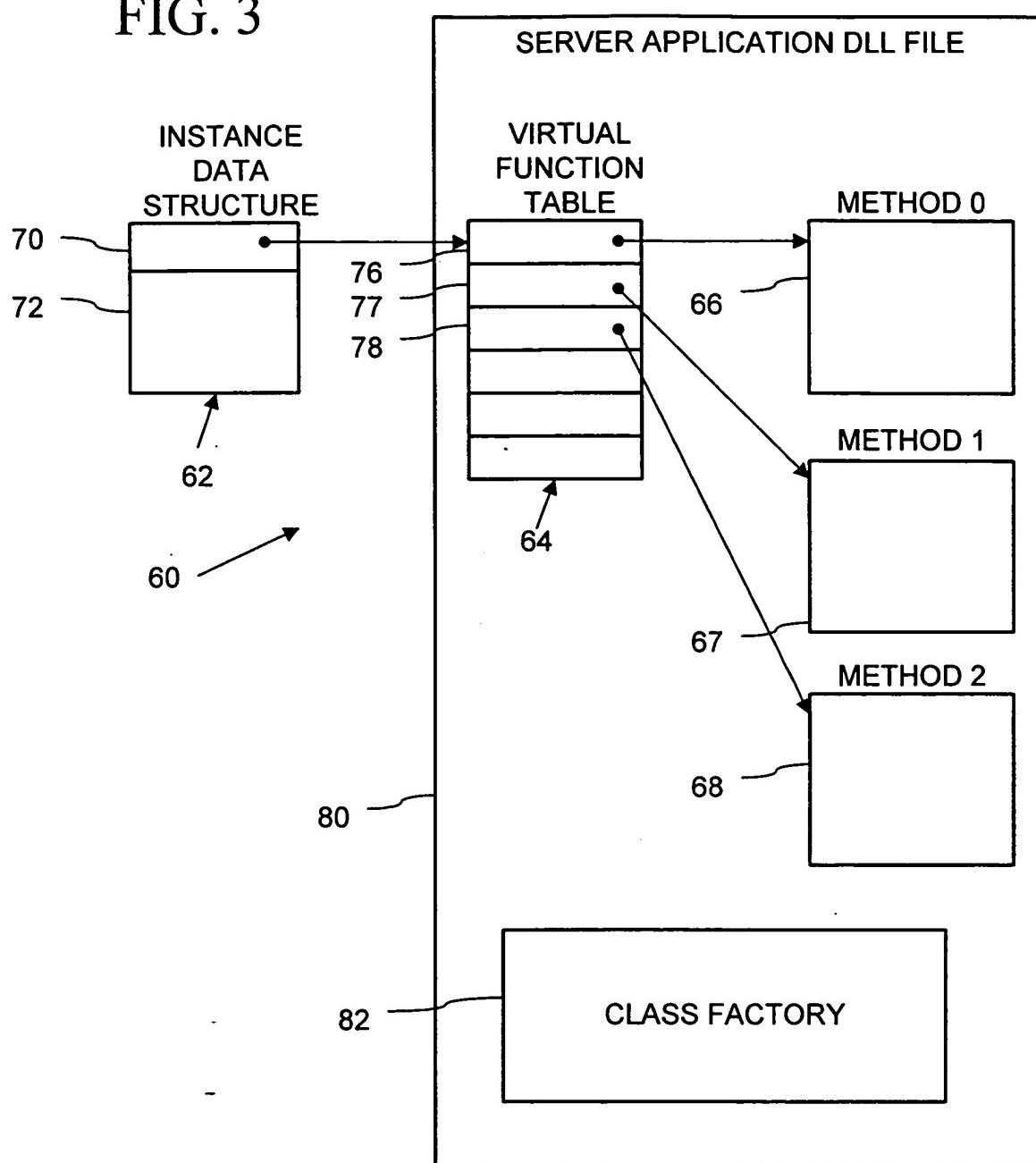


FIG. 3



REF ID OF DRAFTSHEET 50

FIG. 4

DUCTILE TECHNOLOGY

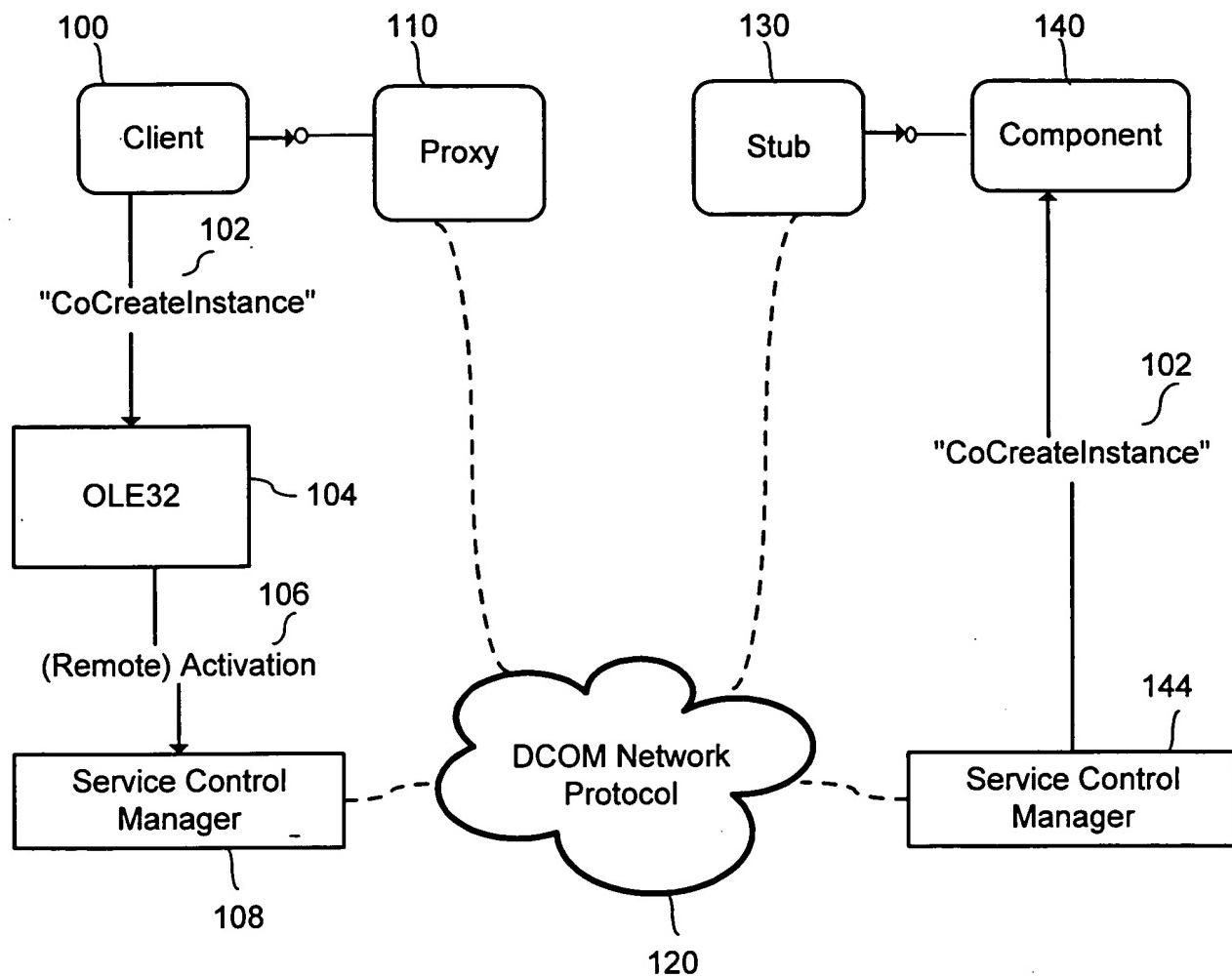
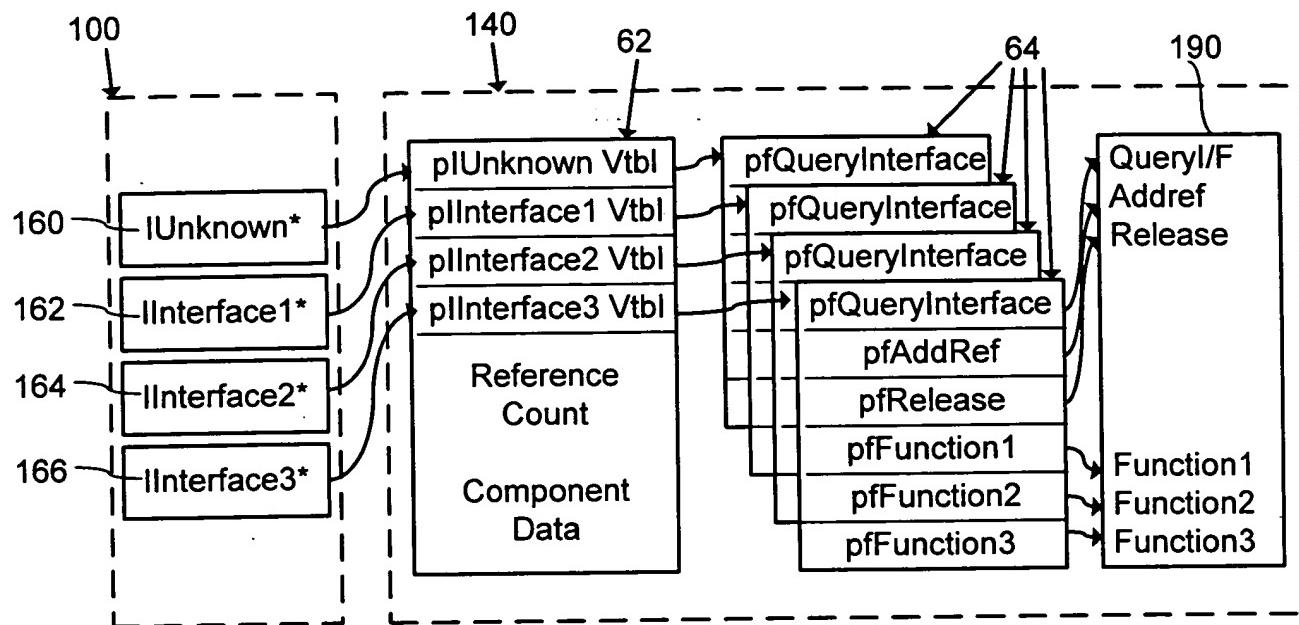


FIG. 5



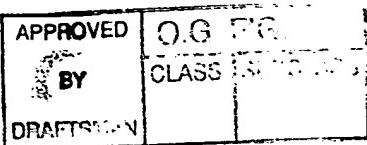
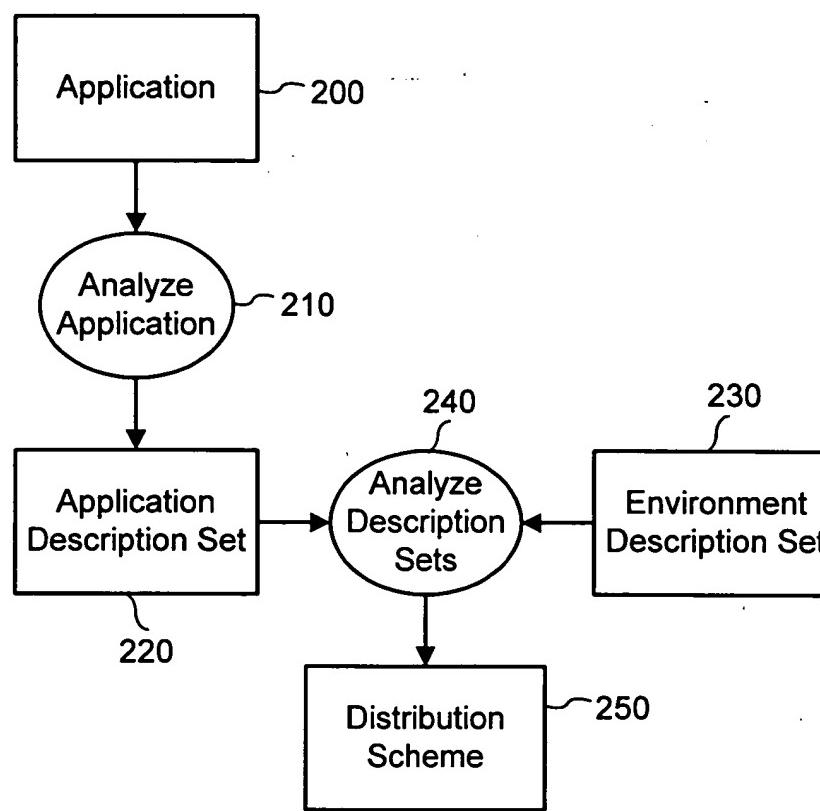
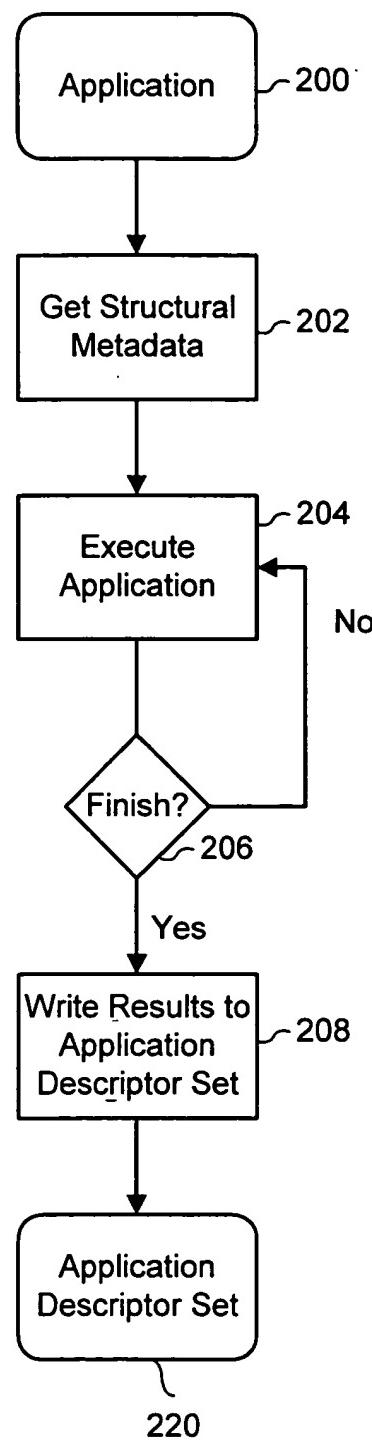


FIG. 6



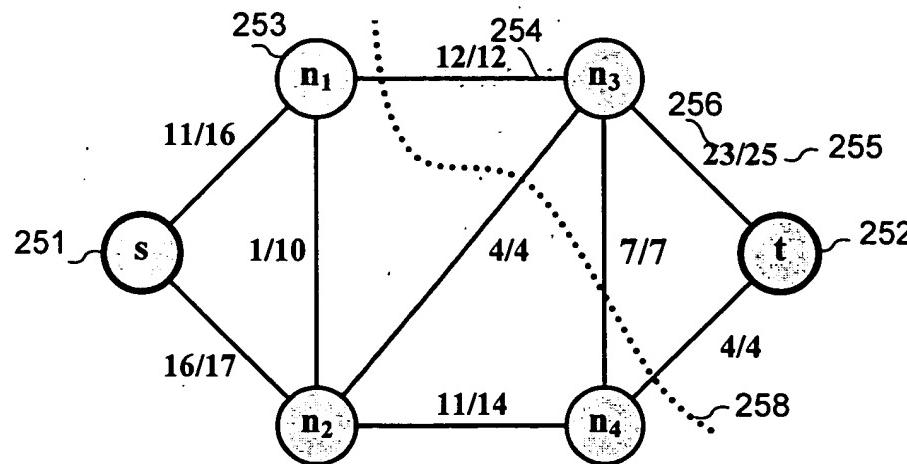
DRAFTSMAN: SPONSOR

FIG. 7



APPROVED	O.G. F.R.
BY	CLASS
DRAFTSMAN	CLASS

FIG. 8



卷之三

APPROVED	Q.C. INC.
BY	CLASS A GROUP
DRAFTED IN	

FIG. 9

260 — Program Control Flow:

```
a.func1: a->func2()  
        ...  
a.func2: b->func3()  
        ...  
b.func3: b->func4()  
        ...  
b.func4: c->func5()  
        ...  
c.func5: CoCreateInstance(type)
```

261 ~ Incremental Classifier:

10 (for 10th call to CoCreateInstance)

262 ~ Component Static-Type Classifier.

## 263 ~ Static-Type Component Call-Chain (T3C) Classifier:

## 264 ~ Procedure Call-Chain (PCC) Classifier:

## 265 ~ Internal Component Call-Chain (I3C) Classifier:

## 266 ~ Entry-point Component Call-Chain (EP3C) Classifier:

# FIG. 10

## // Application Source

...  
 CoCreateInstance (ClSID) → 280 XCoCreateInstance (ClSID)

## :: Application Binary

...  
 push ClSID  
 call [CoCreateInstance] → 281 push ClSID  
 call [XCoCreateInstance]

## :: Application Binary

...  
 CoCreateInstance: → 282 CoCreateInstance:  
 word \_COM\_CoCreateInstance word \_X\_XCoCreateInstance

## :: COM DLL Binary

...  
 \_COM\_CoCreateInstance: → 283 \_COM\_CoCreateInstance:  
 push ebp Call XCoCreateInstance  
 mov ebp, esp push ebp  
 ... mov ebp, esp

## :: COM DLL Binary Replacement

## :: COM DLL Binary

...  
 \_COM\_CoCreateInstance → 284 \_COM\_CoCreateInstance  
 push ebp trap  
 mov ebp, esp mov ebp, esp

## :: COM DLL Binary

...  
 \_COM\_CoCreateInstance → 285 \_COM\_CoCreateInstance  
 push ebp jmp \_X\_XCoCreateInstance  
 mov ebp, esp mov ebp, esp

DECODED BY DR. RAVI KUMAR

FIG. 11

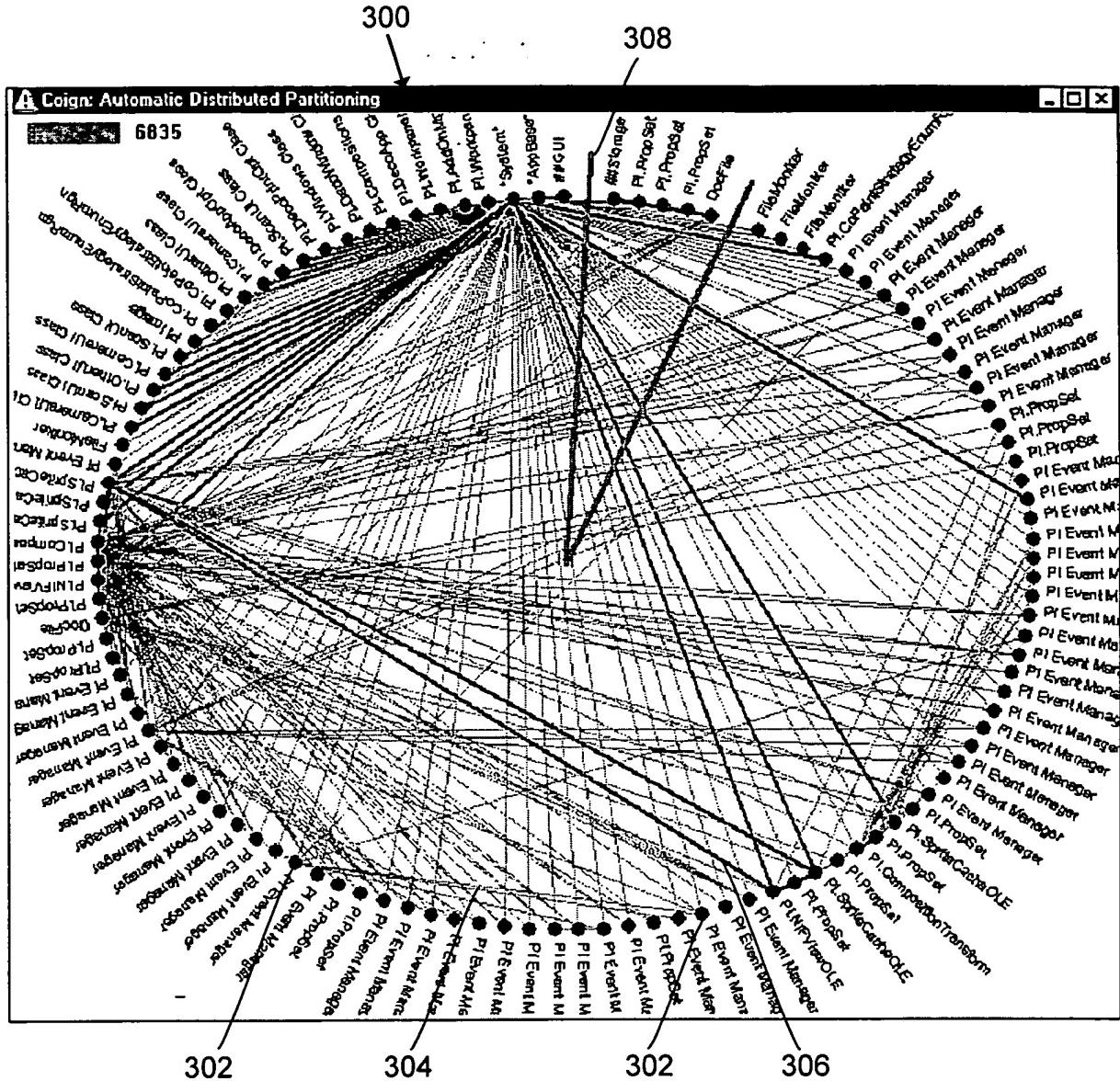
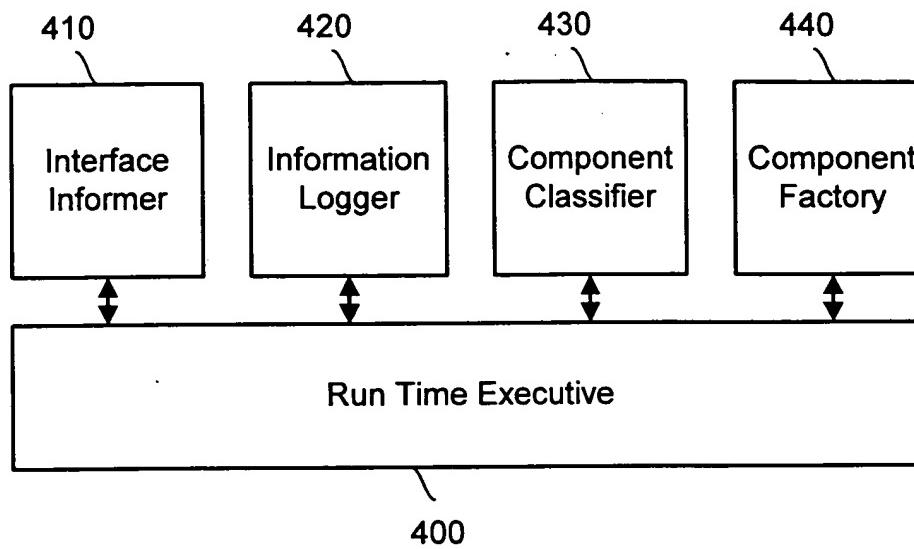
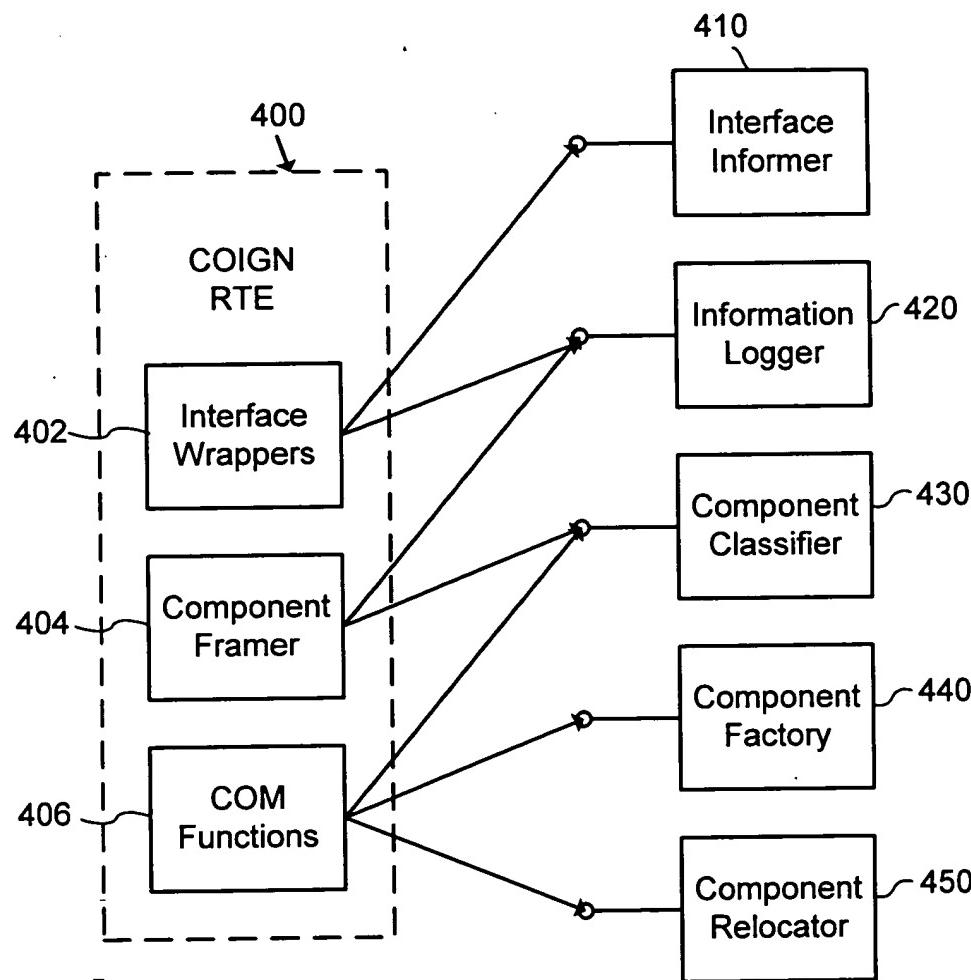


FIG. 12



APPROVED BY	O.C. HQ CLASS SUBCLASS
DRAFTSMAN	

FIG. 13



APPROVED	O.O. FIG.
BY	CLASS 3221AAS
DRAFTSMAN	

FIG. 14

```

;: COM DLL Binary

500 ~ _COM_CoCreateInstance:
    push ebp
    mov  ebp, esp
    502  push ebx
    push esi
    push edi
    ...

;: Trampoline

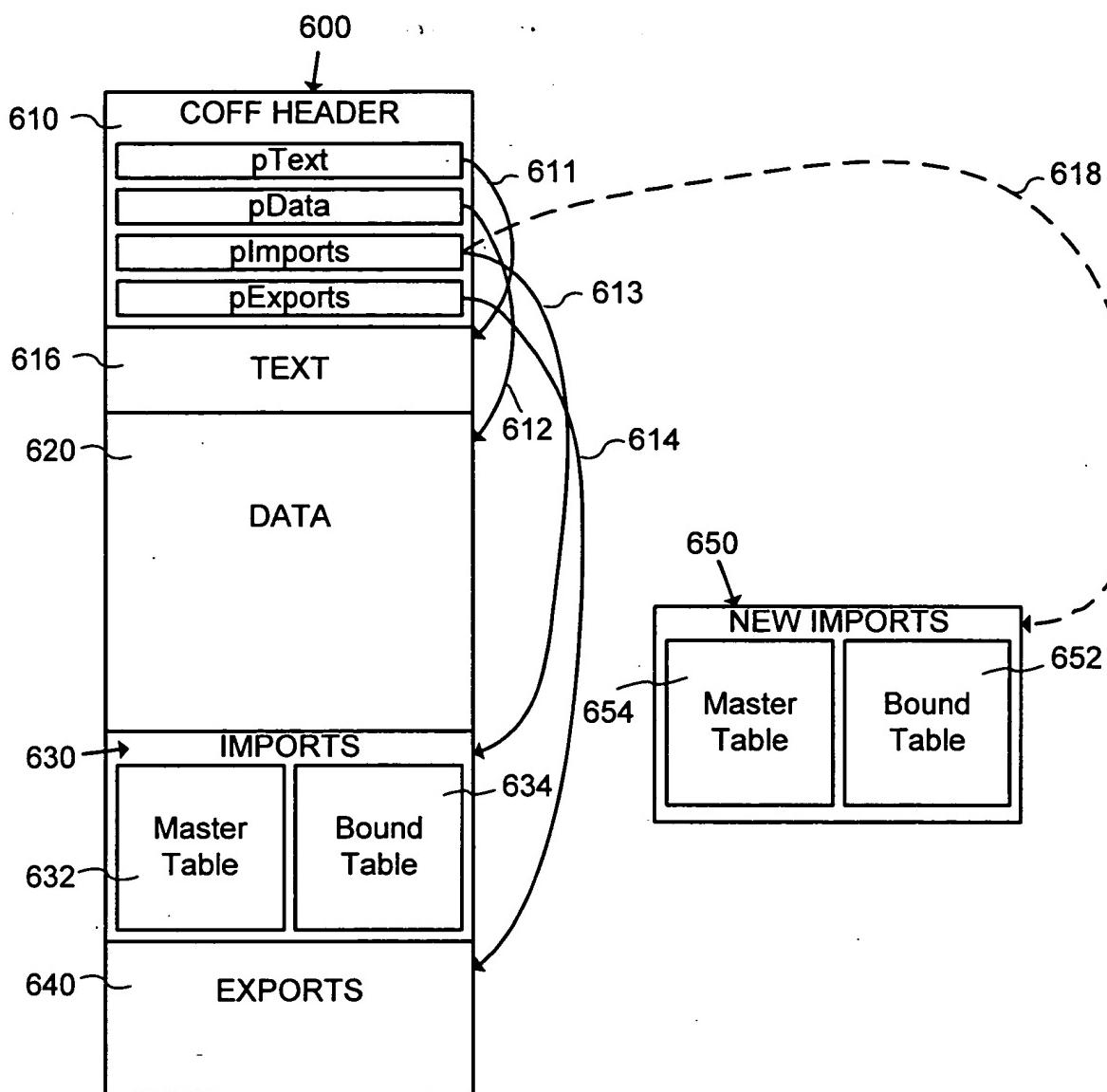
_Trp_CoCreateInstance: ~ 508
    push ebp
    mov  ebp, esp
    502  push ebx
    push esi
    510 ~ jmp  _COM_CoCreateInstance+5
    ...
    501

```

The diagram illustrates a jump from a routine in the COM DLL Binary to a trampoline routine. In the COM DLL Binary section, at address 500, the code pushes EBP onto the stack, moves EBP to ESP, and then pushes EBX, ESI, and EDI onto the stack. An arrow points from this sequence to the Trampoline section at address 508, where the code pushes EBP onto the stack, moves EBP to ESP, and then pushes EBX and ESI onto the stack. The jump instruction at address 510 in the Trampoline section is intended to land at the address of the routine starting at 501 in the COM DLL Binary section.

NOTICE: This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency without the express written permission of the FBI. It and its contents are neither to be quoted nor used without the express written permission of the FBI.

FIG. 15



APPROVED	<input checked="" type="checkbox"/>	BY	CLASS
DRAFTSMAN			SEAL CLASS

FIG. 16

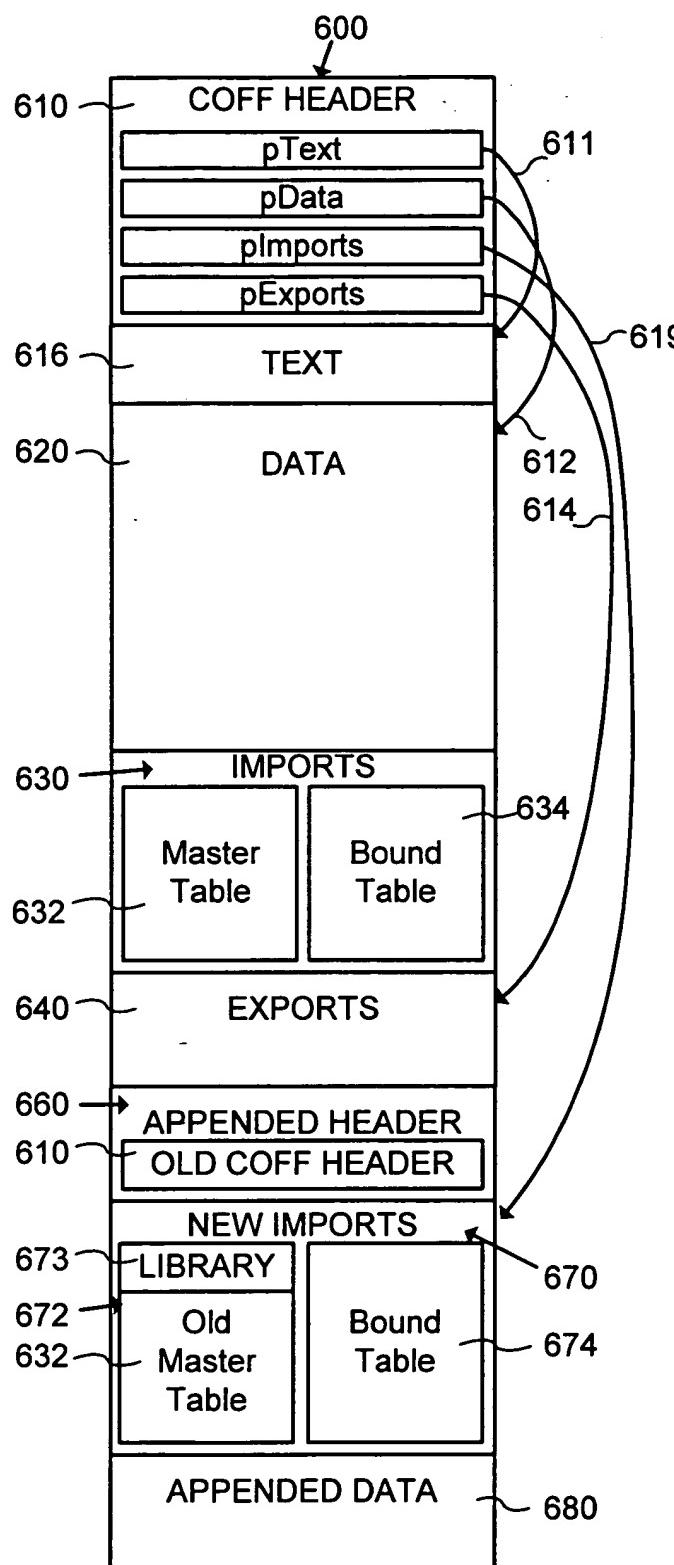


FIG. 17

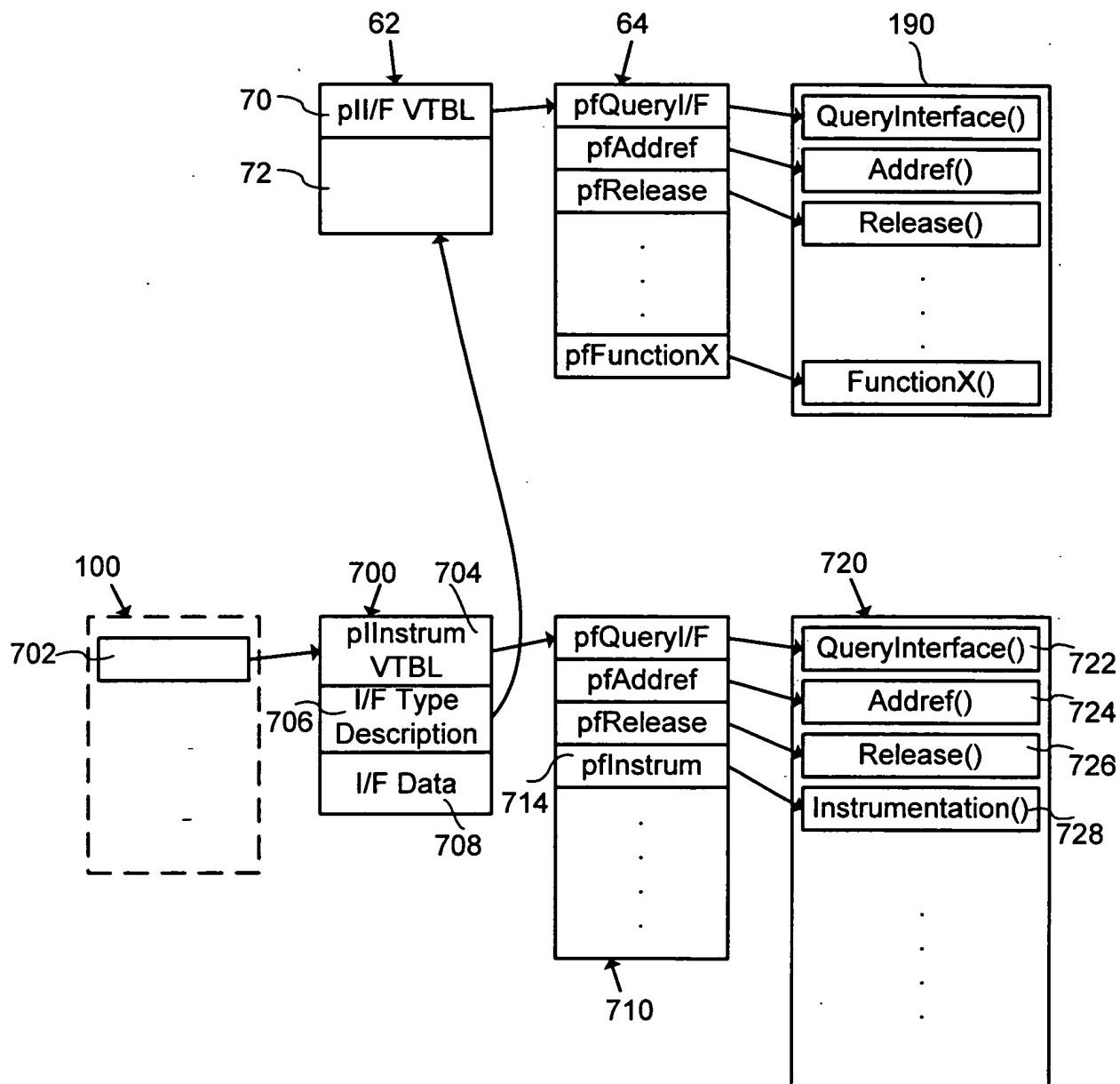
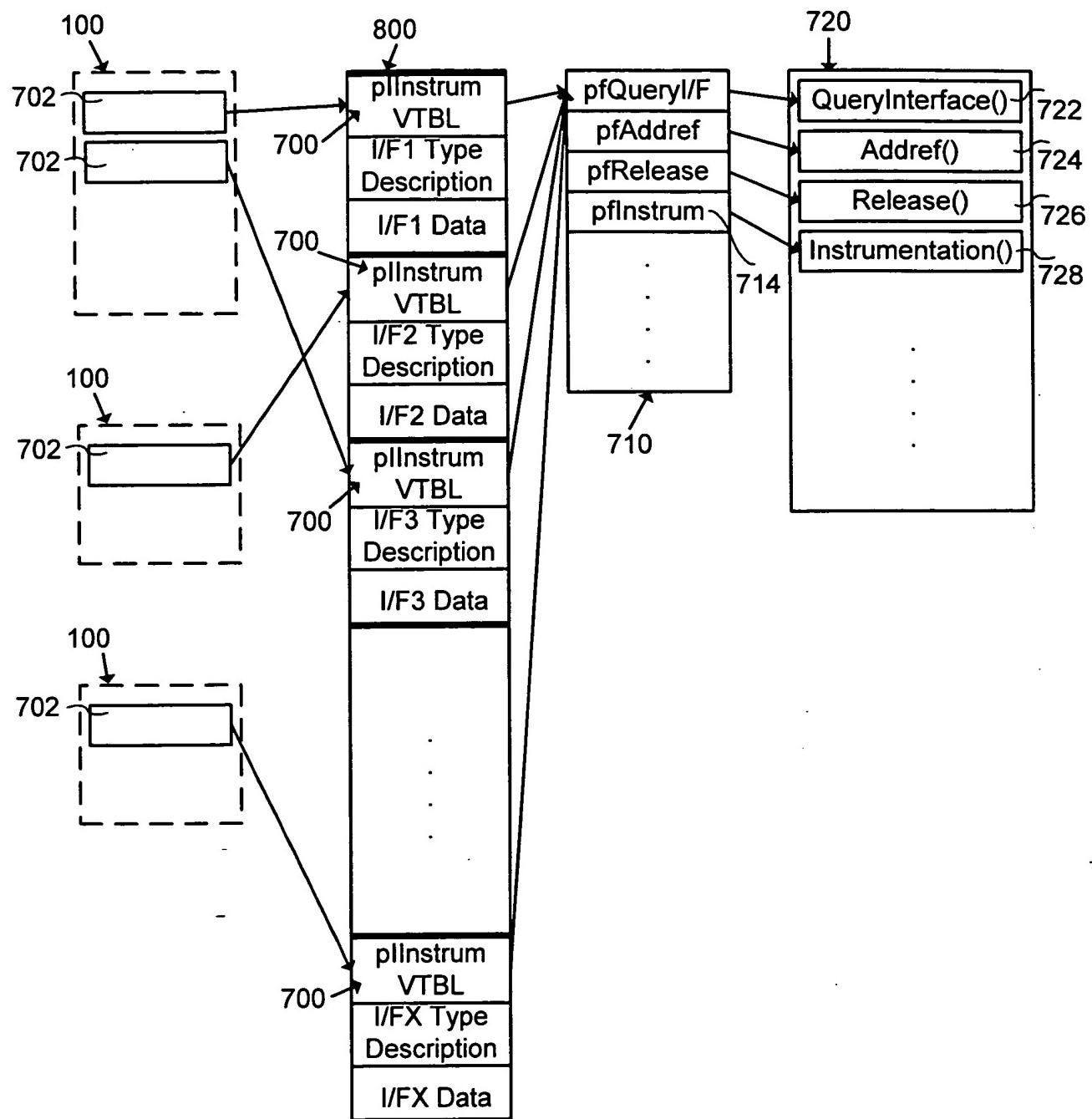


FIG. 18



2020 RELEASE UNDER E.O. 14176